SC01125US00
PA252-US00
②

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: 2００2年 1月30日

出願番号
Application Number: 特願2００2－022360

[ST.10/C]: [JP2００2－022360]

出願人
Applicant(s): 株式会社ソニー・コンピュータエンタテインメント

2００2年 2月22日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号 出証特2００2－3010284

【書類名】　特許願

【整理番号】　SCEI01195

【提出日】　平成14年 1月30日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 12/00

G06F 12/14

【発明者】

【住所又は居所】　東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　久夛良木　健

【発明者】

【住所又は居所】　東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　岡本　伸一

【発明者】

【住所又は居所】　東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　三浦　和夫

【特許出願人】

【識別番号】　395015319

【氏名又は名称】　株式会社ソニー・コンピュータエンタテインメント

【代理人】

【識別番号】　100101867

【弁理士】

【氏名又は名称】　山本　寿武

【先の出願に基づく優先権主張】

【出願番号】　特願2001- 22811

【出願日】　平成13年 1月31日

【整理番号】　SCEI00111

【手数料の表示】

【予納台帳番号】　033466

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9900593

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンピュータシステム及びその使用方法

【特許請求の範囲】

【請求項１】　第１の記録媒体が装着される第１の情報処理装置と、

第１の情報処理装置とネットワークを介して接続される第２の情報処理装置とを備えたネットワークシステムにおいて、

第２の情報処理装置は、

第１の情報処理装置に関連した固有の情報と、第１の記録媒体に関連した固有の情報とを前記第１の情報処理装置から受信し、

第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで記録媒体の認証を行う、ネットワークシステム。

【請求項２】　請求項１に記載のネットワークシステムにおいて、該ネットワークシステムは、更に、

第２の情報処理装置によって、第１の情報処理装置或いは第1の記録媒体に関連した固有の情報をデータベース内に蓄積する、ネットワークシステム。

【請求項３】　請求項１に記載のネットワークシステムは、更に

第２の情報処理装置によって、第１の情報処理装置及び第１の記録媒体に関連した固有の情報をデータベース内に蓄積する、ネットワークシステム。

【請求項４】　請求項１～３のいずれか一項に記載のネットワークシステムにおいて、

データベース内の情報は、予め記録された前記第1の情報処理装置或いは第1の記録媒体に関連した固有の情報である、ネットワークシステム。

【請求項５】　請求項１～３のいずれか一項に記載のネットワークシステムにおいて、

データベース内の情報は、予め記録された前記第1の情報処理装置及び第1の記録媒体に関連した固有の情報である、ネットワークシステム。

【請求項６】　請求項２又は請求項３に記載のネットワークシステムにおいて、

データベース内の情報は、あらたに蓄積された情報に更新される、ネットワークシステム。

【請求項７】　請求項２～６のいずれか一項に記載のネットワークシステムにおいて、

記録媒体が不正に使用された際に、第1の情報処理装置或いは第1の記録媒体に関連した固有の情報をデータベース内に蓄積する、ネットワークシステム。

【請求項８】　請求項１～７のいずれか一項に記載のネットワークシステムは、更に

第２の情報処理装置によって、第１の情報処理装置において実行される処理を可能あるいは不可能とする、ネットワークシステム。

【請求項９】　請求項１～８のいずれか一項に記載のネットワークシステムは、更に

第２の情報処理装置によって、第１の情報処理装置において実行される第１の記録媒体に記録されたプログラムの読取り処理を可能あるいは不可能とする、ネットワークシステム。

【請求項１０】　請求項８又は請求項９に記載のネットワークシステムにおいて、

第２の情報処理装置は、第１の情報処理装置によって実行されるべき処理を可能とする許可信号、あるいは、第１の情報処理装置によって実行されるべき処理を不可能とする拒否信号を送信する、ネットワークシステム。

【請求項１１】　請求項１０に記載のネットワークシステムにおいて、

第２の情報処理装置による参照の結果、データベース内に第１の記録媒体に関連した固有の情報に該当する情報が蓄積されている場合に、第１の情報処理装置によって実行される処理を可能とする、ネットワークシステム。

【請求項１２】　請求項１０に記載のネットワークシステムにおいて、

データベース内には第１の情報処理装置に関連した固有の情報及び第１の記録媒体に関連した固有の情報とが関連付けられた情報として蓄積され、

第２の情報処理装置による参照の結果、第２の情報処理装置が受信した前記第１の情報処理装置に関連した固有の情報及び第１の記録媒体に関連した固有の情

報が、データベース内の関連付けられた情報と一致した場合には、第１の情報処理装置装置によって実行される処理を可能とする、ネットワークシステム。

【請求項１３】　請求項９に記載のネットワークシステムにおいて、

第１の記録媒体にはプログラムが暗号化して記録され、

第２の情報処理装置は、第１の情報処理装置よって暗号化された第１の記録媒体内のプログラムを解読するための情報を送信することで、第１の情報処理装置による第１の記録媒体の読取り処理を可能とする、ネットワークシステム。

【請求項１４】　請求項１３に記載のネットワークシステムにおいて、

解読するための情報は、暗号解読用の鍵である、ネットワークシステム。

【請求項１５】　請求項１～１４のいずれか一項に記載のネットワークシステムは、更に

第１の記録媒体とは異なる第２の記録媒体が装着される第３の情報処理装置に接続され、

第２の情報処理装置によって、第１の情報処理装置から第１の記録媒体に関連する固有の情報を受信すると共に、第３の情報処理装置から第２の記録媒体に関連した固有の情報を受信する、ネットワークシステム。

【請求項１６】　請求項１５に記載のネットワークシステムは、更に、

第２の情報処理装置によって、第１の情報処理装置から受信した第１の記録媒体に関連した固有の情報と、第３の情報処理装置から受信した第２の記録媒体に関連した固有の情報とを参照し、参照した各固有の情報が重複した場合には、第３の情報処理装置において実行される第２の記録媒体に記録されたプログラムの読取り処理を可能あるいは不可能とする、ネットワークシステム。

【請求項１７】　請求項１６に記載のネットワークシステムは、更に

第２の情報処理装置が、第１の情報処理装置に対して、第３の情報処理装置において行われる第２の記録媒体の実行処理を可能にするか否に関して確認情報を送信する、ネットワークシステム。

【請求項１８】　請求項１７に記載のネットワークシステムにおいて

第２の情報処理装置が、第１の情報処理装置から承諾が有った時、第３の情報処理装置において第２の記録媒体の実行処理を可能とする、ネットワークシステ

ム。

【請求項１９】　請求項１～１８のいずれか一項に記載のネットワークシステムにおいて、

第１の情報処理装置には更に第３の記録媒体が装着可能とされ、

第２の情報処理装置は、第１の情報処理装置から受信した第１の情報処理装置に関連した固有の情報及び第１の記録媒体に関連した固有の情報を受信した後に、各固有の情報を第１の情報処理装置に対して送信し、

第１の情報処理装置は各固有の情報を、第２の記録媒体内に蓄積する、ネットワークシステム。

【請求項２０】　請求項１９に記載のネットワークシステムにおいて、更に

第１の情報処理装置は、第１の記録媒体に関連した固有の情報と、第３の記録媒体内に蓄積された情報とを参照する、ネットワークシステム。

【請求項２１】　請求項２０に記載のネットワークシステムにおいて、

第１の情報処理装置による参照の結果、第３の記録媒体内に第１の記録媒体に関連する固有の情報に該当する情報が蓄積されている場合には、第１の情報処理装置によって実行される処理を可能とする、ネットワークシステム。

【請求項２２】　請求項１～２１のいずれか一項に記載の前記ネットワークシステムにおいて、

情報処理装置に関連した固有の情報は機器ＩＤである、ネットワークシステム。

【請求項２３】　請求項１～２２のいずれか一項に記載の前記ネットワークシステムにおいて、

情報処理装置に関連した固有の情報はユーザＩＤである、ネットワークシステム。

【請求項２４】　請求項１～２２のいずれか一項に記載の前記ネットワークシステムにおいて、

前記記録媒体に関連した固有の情報は記録媒体ＩＤである、ネットワークシステム。

【請求項２５】　請求項１に記載のコンピュータシステムにおいて、

前記アプリケーションを記録した記録媒体が光ディスクであり、前記記録媒体ＩＤがディスクＩＤである、コンピュータシステム。

【請求項２６】　請求項２５に記載のコンピュータシステムにおいて、

前記ディスクＩＤは、前記光ディスクのデータエリア内の領域又はデータエリア以外の領域に記録されている、コンピュータシステム。

【請求項２７】　請求項２５に記載のコンピュータシステムにおいて、

前記コンピュータでは、前記ディスクＩＤは、前記光ディスクのデータエリアに記録されたディスクＩＤデータのアドレスに基づき検出される、コンピュータシステム。

【請求項２８】　請求項２５に記載のコンピュータシステムにおいて、

前記ディスクＩＤは、有機色素によりディスクに記録されている、コンピュータシステム。

【請求項２９】　請求項２５に記載のコンピュータシステムにおいて、

前記ディスクＩＤは、ピット列の物理的な変動を利用した方法で形成されている、コンピュータシステム。

【請求項３０】　請求項２９に記載のコンピュータシステムにおいて、

前記ピット列の物理的な変動を利用した方法は、ピット列の半径方向の変動、ピットサイズの短径方向の変動又はピットの深さ方向の変動のいずれかを利用している、コンピュータシステム。

【請求項３１】　請求項２５に記載のコンピュータシステムにおいて、

前記ディスクＩＤは、電子透かしを利用した方法で形成されている、コンピュータシステム。

【請求項３２】　第１の記録媒体が装着される第１の情報処理装置，第１の情報処理装置とネットワークを介して接続される第２の情報処理装置を有するネットワークシステムを利用して、該記録媒体の認証を行う方法において、

第２の情報処理装置が、前記第１の情報処理装置から、第１の情報処理装置に関連した固有の情報と第１の記録媒体に関連した固有の情報とを受信するステップと、

第２の情報処理装置が、第２の情報処理装置に接続或いは含まれ、情報の蓄積

・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第１の記録媒体の認証を行うステップとを含む、方法。

【請求項３３】　第１の記録媒体が装着される第１の情報処理装置であって、第２の情報処理装置とネットワークを介して接続された第１の情報処理装置において、該第１の情報処理装置は、

第１の情報処理装置に関連した固有の情報と第１の記録媒体に関連した固有の情報とを、前記第２の情報処理装置に送信し、

第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第１の記録媒体の認証を行う、第１の情報処理装置。

【請求項３４】　第１の記録媒体が装着される第１の情報処理装置とネットワークを介して接続される第２の情報処理装置において、該第２の情報処理装置は、

第１の情報処理装置に関連した固有の情報と、第１の記録媒体に関連した固有の情報とを前記第１の情報処理装置から受信し、

第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第１の記録媒体の認証を行う、第２の情報処理装置。

【請求項３５】　第１の記録媒体が装着される第１の情報処理装置とネットワークを介して接続される第２の情報処理装置で実行される、該第２の情報処理装置で読み取り可能且つ実行可能なプログラムを記録した記録媒体において、該プログラムは、

第１の情報処理装置に関連した固有の情報と、第１の記録媒体に関連した固有の情報とを前記第１の情報処理装置から受信するステップと、

第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第１の記録媒体の認証を行うステップとを含む、記録媒体。

【請求項３６】　第１の記録媒体が装着される第１の情報処理装置であって、第２の情報処理装置とネットワークを介して接続された第１の情報処理装置で

実行される、該第１の情報処理装置で読み取り可能且つ実行可能なプログラムを記録した記録媒体において、該プログラムは、

第１の情報処理装置に関連した固有の情報と第１の記録媒体に関連した固有の情報とを、前記第２の情報処理装置に送信するステップと、

第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第１の記録媒体の認証を行うステップとを含む、記録媒体。

【請求項３７】　第１の記録媒体が装着される第１の情報処理装置とネットワークを介して接続される第２の情報処理装置で実行される、該第２の情報処理装置で読み取り可能且つ実行可能なプログラムにおいて、

第１の情報処理装置に関連した固有の情報と、第１の記録媒体に関連した固有の情報とを前記第１の情報処理装置から受信するステップと、

第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第１の記録媒体の認証を行うステップとを含む、プログラム。

【請求項３８】　第１の記録媒体が装着される第１の情報処理装置であって、第２の情報処理装置とネットワークを介して接続された第１の情報処理装置で実行される、該第１の情報処理装置で読み取り可能且つ実行可能なプログラムにおいて、

第１の情報処理装置に関連した固有の情報と第１の記録媒体に関連した固有の情報とを、前記第２の情報処理装置に送信するステップと、

第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第１の記録媒体の認証を行うステップとを含む、プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムに関する。

【０００２】

【従来の技術】

光ディスクを装着して使用するコンピュータでは、各種のプログラムを実行することが出来る。このようなコンピュータの一つにエンタテインメントシステムがあり、代表的にはゲーム装置として使用されている。このようなエンタテインメントシステムでは、ゲームプログラムが記録された光ディスクを購入し、ゲームを実行する。また最近、エンタテインメントシステムは、ネットワークを介して、多数のゲームプログラムを蓄積したコンテンツサーバと接続され、ゲームプログラムをネットワークを介してダウンロードして購入するようなことも計画されている。

【０００３】

【発明が解決しようとする課題】

購入された光ディスク又はダウンロードしたプログラムを記録した光ディスクが、不正に使用される場合がある。即ち、プログラムを記録した光ディスクが、プログラムに関する著作権者の許可無く、不正にコピーされたり、これを中古品として販売されたりすることがある。このような状態を放置すると、著作権者は正当な利益を回収することが出来ず、プログラム創作の意欲が削がれることになる。

【０００４】

【課題を解決するための手段】

上述の問題点に鑑みて、本発明は、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムを有するコンピュータシステムを提供することを目的とする。

【０００５】

更に、本発明は、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムを有するコンピュータシステムの使用方法を提供することを目的とする。

【０００６】

本発明に係るネットワークシステムは、第１の記録媒体（例えば、光ディスク

）が装着される第１の情報処理装置（例えば、一のエンタテイメント装置）と、第１の情報処理装置とネットワークを介して接続される第２の情報処理装置（例えば、認証用サーバ）とを備えたネットワークシステムであって、第２の情報処理装置は、第１の情報処理装置に関連した固有の情報（例えば、機器ＩＤ）と、第１の記録媒体に関連した固有の情報とを前記第１の情報処理装置から受信し、第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで記録媒体の認証を行う。

【０００７】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、該ネットワークシステムは、更に、第２の情報処理装置によって、第１の情報処理装置或いは第１の記録媒体に関連した固有の情報をデータベース内に蓄積する。

【０００８】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第２の情報処理装置によって、第１の情報処理装置及び第１の記録媒体に関連した固有の情報をデータベース内に蓄積する。

【０００９】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、データベース内の情報は、予め記録された前記第１の情報処理装置或いは第１の記録媒体に関連した固有の情報である。

【００１０】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、データベース内の情報は、予め記録された前記第１の情報処理装置及び第１の記録媒体に関連した固有の情報である。

【００１１】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、データベース内の情報は、あらたに蓄積された情報に更新される。

【００１２】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、記録媒体が不正に使用された際に、第１の情報処理装置或いは第１の記録媒体に関連した固有の情報をデータベース内に蓄積する。

【００１３】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第２の情報処理装置によって、第１の情報処理装置において実行される処理を可能あるいは不可能とする。

【００１４】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第２の情報処理装置によって、第１の情報処理装置において実行される第１の記録媒体に記録されたプログラムの読取り処理を可能あるいは不可能とする。

【００１５】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第２の情報処理装置は、第１の情報処理装置によって実行されるべき処理を可能とする許可信号、あるいは、第１の情報処理装置によって実行されるべき処理を不可能とする拒否信号を送信する。

【００１６】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第２の情報処理装置による参照の結果、データベース内に第１の記録媒体に関連した固有の情報に該当する情報が蓄積されている場合に、第１の情報処理装置によって実行される処理を可能とする。

【００１７】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、データベース内には第１の情報処理装置に関連した固有の情報及び第１の記録媒体に関連した固有の情報とが関連付けられた情報として蓄積され、第２の情報処理装置による参照の結果、第２の情報処理装置が受信した前記第１の情報処理装置に関連した固有の情報及び第１の記録媒体に関連した固有の情報が、データベース内の関連付けられた情報と一致した場合には、第１の情報処理装置

によって実行される処理を可能とする。

【００１８】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第１の記録媒体にはプログラムが暗号化して記録され、第２の情報処理装置は、第１の情報処理装置よって暗号化された第１の記録媒体内のプログラムを解読するための情報を送信することで、第１の情報処理装置による第１の記録媒体の読取り処理を可能とする。

【００１９】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、解読するための情報は、暗号解読用の鍵である。

【００２０】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第１の記録媒体とは異なる第２の記録媒体（例えば、光ディスク）が装着される第３の情報処理装置（例えば、他のエンタテイメント装置）に接続され、第２の情報処理装置によって、第１の情報処理装置から第１の記録媒体に関連する固有の情報を受信した後に、第３の情報処理装置から第２の記録媒体に関連した固有の情報を受信する。

【００２１】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第２の情報処理装置によって、第１の情報処理装置から受信した第１の記録媒体に関連した固有の情報と、第３の情報処理装置から受信した第２の記録媒体に関連した固有の情報とを参照し、参照した各固有の情報が重複した場合には、第３の情報処理装置において実行される第２の記録媒体に記録されたプログラムの読取り処理を可能あるいは不可能とする。

【００２２】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第２の情報処理装置が、第１の情報処理装置に対して、第３の情報処理装置において行われる第２の記録媒体の実行処理を可能にするか否に関して確認情報を送信する。

【００２３】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第１の情報処理装置から承諾が有った時、第３の情報処理装置において第２の記録媒体の実行処理を可能とする。

【００２４】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第１の情報処理装置には更に第３の記録媒体（例えば、メモリカード）が装着可能とされ、第２の情報処理装置は、第１の情報処理装置から受信した第１の情報処理装置に関連した固有の情報及び第１の記録媒体に関連した固有の情報を受信した後に、各固有の情報を第１の情報処理装置に対して送信し、第１の情報処理装置は各固有の情報を、第２の記録媒体内に蓄積する。

【００２５】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第１の情報処理装置は、第１の記録媒体に関連した固有の情報と、第３の記録媒体内に蓄積された情報とを参照する。

【００２６】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第１の情報処理装置による参照の結果、第３の記録媒体内に第１の記録媒体に関連する固有の情報に該当する情報が蓄積されている場合には、第１の情報処理装置によって実行される処理を可能とする。

【００２７】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、情報処理装置に関連した固有の情報は機器ＩＤである。

【００２８】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、情報処理装置に関連した固有の情報はユーザＩＤである。

【００２９】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記記録媒体に関連した固有の情報は記録媒体ＩＤである。

【００３０】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記アプリケーションを記録した記録媒体が光ディスクであり、前記記録媒体ＩＤがディスクＩＤである。

【００３１】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ディスクＩＤは、前記光ディスクのデータエリア内の領域又はデータエリア以外の領域に記録されている。

【００３２】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記コンピュータでは、前記ディスクＩＤは、前記光ディスクのデータエリアに記録されたディスクＩＤデータのアドレスに基づき検出される。

【００３３】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ディスクＩＤは、有機色素によりディスクに記録されている。

【００３４】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ディスクＩＤは、ピット列の物理的な変動を利用した方法で形成されている。

【００３５】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ピット列の物理的な変動を利用した方法は、ピット列の半径方向の変動、ピットサイズの短径方向の変動又はピットの深さ方向の変動のいずれかを利用している。

【００３６】

更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ディスクＩＤは、電子透かしを利用した方法で形成されている。

【００３７】

更に、本発明に係る記録媒体の認証を行う方法は、第１の記録媒体が装着され

る第１の情報処理装置，第１の情報処理装置とネットワークを介して接続される第２の情報処理装置を有するネットワークシステムを利用して、該記録媒体の認証を行う方法であって、第２の情報処理装置が、前記第１の情報処理装置から、第１の情報処理装置に関連した固有の情報と第１の記録媒体に関連した固有の情報とを受信するステップと、第２の情報処理装置が、第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで記録媒体の認証を行うステップとを含む。

【００３８】

更に、本発明に係る第１の情報処理装置は、第１の記録媒体が装着される第１の情報処理装置であり、第２の情報処理装置とネットワークを介して接続された第１の情報処理装置であって、該第１の情報処理装置は、第１の情報処理装置に関連した固有の情報と第１の記録媒体に関連した固有の情報とを、前記第２の情報処理装置に送信し、第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第１の記録媒体の認証を行う。

【００３９】

更に、本発明に係る第２の情報処理装置は、第１の記録媒体が装着される第１の情報処理装置とネットワークを介して接続される第２の情報処理装置であって、該第２の情報処理装置は、第１の情報処理装置に関連した固有の情報と、第１の記録媒体に関連した固有の情報とを前記第１の情報処理装置から受信し、第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第１の記録媒体の認証を行う。

【００４０】

更に、本発明に係る記録媒体は、第１の記録媒体が装着される第１の情報処理装置とネットワークを介して接続される第２の情報処理装置で実行される、該第２の情報処理装置で読み取り可能且つ実行可能なプログラムを記録した記録媒体であって、該プログラムは、第１の情報処理装置に関連した固有の情報と、第１の記録媒体に関連した固有の情報とを前記第１の情報処理装置から受信するステ

ップと、第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第１の記録媒体の認証を行うステップとを含む。

【００４１】

更に、本発明に係るプログラムは、第１の記録媒体が装着される第１の情報処理装置であって、第２の情報処理装置とネットワークを介して接続された第１の情報処理装置で実行される、該第１の情報処理装置で読み取り可能且つ実行可能なプログラムを記録した記録媒体であって、該プログラムは、第１の情報処理装置に関連した固有の情報と第１の記録媒体に関連した固有の情報とを、前記第２の情報処理装置に送信するステップと、第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第１の記録媒体の認証を行うステップとを含む。

【００４２】

更に、本発明に係るプログラムは、第１の記録媒体が装着される第１の情報処理装置とネットワークを介して接続される第２の情報処理装置で実行される、該第２の情報処理装置で読み取り可能且つ実行可能なプログラムであって、該プログラムは、第１の情報処理装置に関連した固有の情報と、第１の記録媒体に関連した固有の情報とを前記第１の情報処理装置から受信するステップと、第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第１の記録媒体の認証を行うステップとを含む。

【００４３】

更に、本発明に係るプログラムは、第１の記録媒体が装着される第１の情報処理装置であって、第２の情報処理装置とネットワークを介して接続された第１の情報処理装置で実行される、該第１の情報処理装置で読み取り可能且つ実行可能なプログラムであって、該プログラムは、第１の情報処理装置に関連した固有の情報と第１の記録媒体に関連した固有の情報とを、前記第２の情報処理装置に送信するステップと、第２の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで

第１の記録媒体の認証を行うステップとを含む。

【００４４】

【発明の実施の形態】

以下、添付の図面を参照しながら本実施形態について詳細に説明する。

[ディスク認証システム]

（システム全体）

図１は、本実施例に係るディスク認証システム全体の概念図である。図１に示されるように、ユーザ端末機器１が、ネットワーク３を介して認証用サーバ４と接続されている。この認証用サーバ４は、ネットワーク３を介して１又は２以上のコンテンツサーバ６と接続されている。これらのコンテンツサーバ６にはデバッグ専用サーバ６－４があってもよい。

【００４５】

ユーザ端末機器１は、アプリケーションプログラムを記録したＣＤ－ＲＯＭ（Compact Disc-Read Only Memory）、ＤＶＤ－ＲＯＭ（Digital Versatile Disc-ROM）等の光ディスク２を搭載可能なコンピュータである。本実施例では、ゲーム機等に代表されるエンタテインメントシステムを例にとって説明する。このユーザ端末機器１はエンタテインメント本体装置に該当し、エンタテインメント本体装置に関しては、後で図２を用いてその内部の構成を説明する。なお、光ディスク２は、例示であって、これに限定されない。アプリケーションプログラム等のコンテンツを記録した種々の記録媒体全てが対象となることを承知されたい。例えば、外部接続のハードディスク（図示せず。）、後述のコネクタに接続されるメモリカード又はＰＤＡ内のメモリ等にアプリケーションプログラム等のコンテンツが記録されている場合には、これらは対象となる。しかし、説明を分かり易くするため、光ディスク２を例にとって説明する。

【００４６】

ネットワーク３としては、テレビジョンケーブルネットワーク、光ファイバネットワーク、ｘＤＳＬ（x Digital Subscriber Line）等のいわゆるブロードバンドネットワークが好ましい。また、既存の又はこれから構築される広帯域無線ネットワーク、携帯電話及びＰＨＳ（Pers nal Handyph ne System）電話関連の

ネットワーク、インターネット関連のネットワーク等も利用することができる。

【００４７】

認証用サーバ４は、エンタテインメント装置１に接続され、エンタテインメント装置１及び記録媒体２が真正であるか不正であるかの認証を行うために用いられるサーバである。認証用サーバ４は、各々のエンタテインメント本体装置１に付与された固有のＩＤである機器ＩＤ（「ＳＥＴ　ＩＤ」とも言う。）情報と、各々のユーザに付与された固有のＩＤであるユーザＩＤ（「ＵＳＥＲ　ＩＤ」とも言う。）情報（パスワードを含む場合もある。）と、各々の光ディスク２に付与された固有のＩＤであるディスクＩＤ（「ＤＩＳＫ　ＩＤ」とも言う。）等のユーザ情報を蓄積するユーザデータベース５を有する。これらのＩＤは、各々単一なものであり、同じＩＤは２つ以上存在しない。特に、ディスクＩＤは、光ディスク１枚毎に付された相異なる識別記号である。

【００４８】

また、コンテンツサーバ６は、ユーザに提供し得る種々のディジタルコンテンツを蓄積したデータベース７を夫々有している。

【００４９】

更に、認証用サーバ４の代わりに、エンタテインメント装置１を用いることもできる。即ち、複数のエンタテインメント装置１が接続されて、その内の特定の一台が認証用サーバの役割を果たす場合である。この場合、これに接続されるユーザデータベース５は、ハードディスクのような記録媒体で構成される。

【００５０】

（装置本体の内部構成）

図２は、図１のユーザ端末として利用されるエンタテインメントシステムの本体装置の内部構成のブロック図である。図中、一点鎖線内はエンタテインメント本体装置１を、破線内は該エンタテインメント本体装置１のディスクドライブ３０を、夫々示している。

【００５１】

エンタテインメント本体装置１はＣＰＵ１６を有し、このＣＰＵ１６はメインメモリ（ＲＡＭ）１７と接続されている。また、ＣＰＵ１６は描画装置（ＧＰＵ

）１８と接続されており、ＧＰＵ１８からの映像信号は、ＣＲＴ－ＣＴＲ（Cath de Ray Tube-Contr l）（図示せず。）を介して表示装置（ＣＲＴ）（図示せず。）に出力されている。また、ＣＰＵ１６は、ＵＳＢ（Universal Serial Bus）コネクタ１４、ＩＥＥＥ１３９４又はｉリンク（i.LINK（登録商標））コネクタ１５等を有するＩＯＰ（Input/Output Processor）１３を介して、コネクタ（コントローラ（ＰＡＤ）／ＰＤＡ（Personal Digital Assistant）／メモリカード・コネクタ）１２に接続されている。

【００５２】

このコネクタ１２には、メモリカード１１、コントローラ（ＰＡＤ）１０、携帯端末（ＰＤＡ：Personal Digital Assistant）等が接続される。このメモリカード１１、ＰＤＡ等は、外部記憶装置の一種であり、後述するように、ディスクＩＤ、機器ＩＤ等が記録される。

【００５３】

また、ＣＰＵ１６は、ＩＯＰ１３を介してバス２７に接続され、このバス２７には、ＭＡＳＫ－ＲＯＭ（Masked ROM）１９、ＣＤ／ＤＶＤ－ＤＳＰ（CD/DVD-Digital Signal Processor）２２、ＤＶＤプレイヤＲＯＭ２０、ＳＰＵ（Sound Processing Unit）２５、ネットワーク・インターフェース２６等が接続されている。ＳＰＵ２５からの音声信号は、アンプ、スピーカ等（図示せず。）に出力されている。エンタテインメント本体装置１は、ネットワーク・インターフェース２６、ＵＳＢコネクタ１４、ｉリンクコネクタ１５等を介してネットワークと接続され、更にネットワークを通じて認証用サーバ４、デジタルコンテンツサーバ６等に接続される。

【００５４】

ＣＤ／ＤＶＤ－ＤＳＰ２２は、メカニカル制御部２３及びドライバ２４を介して、ディスクドライブ３０の機械的制御を行う。この制御は、ＲＦ－ＡＭＰ（Radio Frequency Amplifier）２１を通じて行われる。また、ＣＤ／ＤＶＤ－ＤＳＰ２２は、ＲＦ－ＡＭＰ２１を通じて、ディスクドライブ３０の電気的制御を行う。

【００５５】

光ディスク２は、スピンドルモータ（図示せず。）の機械的制御により回転される。また、光ディスク２に対しては、アクチュエータ（図示せず。）の電気的制御によりピックアップレンズ（図示せず。）が駆動されて情報の記録／再生が行われる。

【００５６】

このエンタテインメント装置１は、製造番号等の固有のＩＤである機器ＩＤを有している。この機器ＩＤは、例えば予めマスクＲＯＭ１９に書き込まれるようにハードウェア的に組み込まれたもの、或いは後から光ディスク２，メモリカード１１，携帯端末，コントローラ１０等を介してソフトウェア的に読み込まれたもの、のいずれでもよい。

【００５７】

また、この光ディスク２にはディスクＩＤが記録されており、このディスクＩＤは後述する方法で読み取られる。

［ディスクＩＤ認証システム］

（第１のディスクＩＤ認証システム）

以下、図３を用いて第１のディスクＩＤ認証システムのエンタテインメント本体装置側の処理に関して具体的に説明し、図４を用いて認証用サーバ４側の処理に関して具体的に説明する。なお、本実施例においては、エンタテインメントシステムはゲーム機であり、ゲームプログラムを記憶した記録媒体としてはＣＤ－ＲＯＭのような光ディスクを使用し、更にディスクＩＤが通常のデータエリア以外のエリア（例えば、リードインエリアの内側、リードアウトの外側等）に存在する場合を前提として説明する。

【００５８】

図３は、エンタテインメント本体装置側の処理を示している。まず、エンタテインメント本体装置における処理の基本を説明する。ここで使用されている光ディスクは、通常では記録対象となっていないエリアにディスクＩＤが記録されている。このディスクＩＤの記録箇所を特定する情報（例えば、アドレス）は、通常のデータエリアに記録されている。光ディスク２にディスクＩＤを記入するための材料としては、追記型ディスクに使用されている有機色素が一例として挙げ

られる。エンタテインメント本体装置は、ディスク情報を読み取り、そこからディスクＩＤの記録されたアドレスを検索し、更にこのアドレスに従ってディスクＩＤを読み取り、それを認証用サーバ４に送信している。以下、具体的に説明する。

【００５９】

ステップS102において、エンタテインメント本体装置１は、ＣＰＵの制御のもと、搭載されたＣＤ－ＲＯＭからＴＯＣ（Table of Contents）の基礎データを読み込む。そして、ステップS103において、ＣＤ－ＲＯＭのデータエリアのボリューム識別子ＶＤ（Volume Description）を読み込み、ディスクＩＤの記入してあるアドレスを検索する。

【００６０】

ステップS104では、ボリューム識別子ＶＤにディスクＩＤのアドレスが存在するか否かが判定される。ＩＤのアドレスが存在しなければ、搭載されたＣＤ－ＲＯＭは、このディスクＩＤ認証システムによる保護対象以外のＣＤ－ＲＯＭと判定され、ステップS113に進行し、プログラムが実行される。このエンタテインメント本体装置１は、単にゲーム機として機能するだけでなく、音楽用ＣＤ再生装置、映画用ＤＶＤ再生装置等としても機能する。このため、エンタテインメント本体装置に、ＩＤ認証システムによる保護対象以外の光ディスク（例えば、ＤＶＤ－Ｖｉｄｅｏ、Ａｕｄｉｏ－ＣＤ、従来のゲームＣＤ等）が搭載されている場合があり、このような場合はそのまま音楽や映像の再生やゲームの実行が行われる。

【００６１】

ボリューム識別子ＶＤにＩＤアドレスが存在する場合、ステップS105において、ディスクＩＤを読み取るために、ＩＤアドレスに従って光ディスクドライブ３０のピックアップをＣＤ－ＲＯＭのディスクＩＤデータ部（リードインエリア内側又はリードアウトの外側に設けられた部分）に向けてスライドさせる。このピックアップのスライド制御は、ＣＰＵ１６から出力されたスライド命令に基づいて、メカニカル制御部２３にて行われる。

【００６２】

ステップS106において、ＣＰＵ１６は、ＣＤ－ＲＯＭ上のディスクＩＤデータ部に、実際にディスクＩＤ情報が存在するか否かを判別する。ディスクＩＤ情報が存在しない場合又はディスクＩＤ情報の読込みが不可能な場合には、ディスクＩＤ無しと判定され、ステップS107に進む。このステップS107では、プログラムの実行は拒否され、強制終了される。

【００６３】

ディスクＩＤデータ部に実際にディスクＩＤ情報が存在する場合、エンタテインメント本体装置１は、ステップS108において、ＣＰＵの制御の下、ディスクＩＤ情報を読み取りこれをメインメモリ１７に記憶する。

【００６４】

ステップS109において、エンタテインメント本体装置１のＣＰＵ１６は、ディスクＩＤのデータを、ＵＳＢ、ＩＥＥＥ（Institute of Electrical and Electronic Engineers）１３９４、ＰＣＭＣＩＡ（Personal Computer Memory Card International Association Architecture）等の規格に準拠した各種通信インターフェイスを介して、認証用サーバ４に対して送信する。そして、ステップS110で、送信したディスクＩＤに対して認証用サーバが認証処理を行うのを待つ。

【００６５】

ステップS111において、エンタテインメント本体装置１は、認証用サーバでの認証処理結果を受信する。認証用サーバでの認証処理の結果が「認証適」であれば、ＣＤ－ＲＯＭの読み取り許可命令が受信される。認証処理の結果が「認証否」であればステップS112に進み、プログラムの実行が拒否されて強制終了される。

【００６６】

認証用サーバでの認証処理の結果が「認証適」の場合、ステップS113において、エンタテインメント本体装置１のＣＰＵは、ＣＤ－ＲＯＭに記録されたプログラムを実行する。

【００６７】

図４は、第１のディスクＩＤ認証システムにおける認証用サーバ４側の処理を示している。まず、認証用サーバ４における処理の基本を説明する。エンタテイ

ンメント本体装置１を購入したユーザは、その直後に、自分の氏名等のユーザＩＤと、各本体機器に付与された機器ＩＤとを認証用サーバ４のユーザデータベース５に登録している。また、新たなゲームプログラムを購入したユーザは、その最初の使用時にディスクＩＤ情報を認証用サーバ４のユーザデータベース５に送信しなければ、そのプログラムの実行が出来ない（ステップS109参照）。このため、認証用サーバ４のユーザデータベース５には、ユーザ情報として、少なくともディスクＩＤと、更に、これと関連するユーザＩＤ，機器ＩＤ等の任意のものが蓄積される。ユーザ情報は、ユーザが複数の種類のゲームプログラムを購入すると、１つのユーザＩＤ及び機器ＩＤに対して複数のディスクＩＤの組み合わせとなる。ユーザ情報は、テーブル化されてユーザデータベース５に蓄積される。

【００６８】

このような状況下で、ユーザがゲームを開始する場合、ユーザが使用しているディスクＩＤと機器ＩＤの情報が、エンタテインメント本体機器１から認証用サーバ４に送信され、認証用サーバ４のユーザデータベースに蓄積されたユーザ情報と比較される。この比較結果は、図７に示すように、次の４通りとなる。

【００６９】

(No.1)ディスクＩＤと機器ＩＤの両方が、蓄積されたものと一致する。

【００７０】

(No.2)ディスクＩＤのみが、蓄積されたものと一致する。

【００７１】

(No.3)機器ＩＤのみが、蓄積されたものと一致する。

【００７２】

(No.4)ディスクＩＤと機器ＩＤのいずれも、蓄積されたものとは一致しない。

【００７３】

Ｎｏ．１の、送信されたディスクＩＤと機器ＩＤの組み合わせが、既にユーザデータベースに登録されたこれらに対応する情報と一致した場合、このディスクは正規のディスクと判断される。しかし、希なケースとして、機器ＩＤが不正にコピーされ、且つディスクＩＤも不正にコピーされたような場合が起こる可能性がある。このようなケースを排除するため、同一のディスクＩＤと機器ＩＤの組

み合わせの認証要求が、同じ時間帯に重複した場合は不正使用であると判断し、この不正使用をカウントしてユーザデータベース５に記録すると共に、プログラムの実行を拒否する。

【００７４】

Ｎｏ．２の、送信されたディスクＩＤと機器ＩＤの組み合わせの内、ディスクＩＤのみがデータベースに蓄積されたものと一致した場合、次の３通りの状況が考えられる。

【００７５】

(1)ディスク所有者が自分のディスクを他人に貸与した場合

(2)ディスク所有者が自分のディスクを他人の機器で実行した場合

(3)不正コピーの場合

これらのいずれに該当するかは、ディスクＩＤと共に登録されている機器ＩＤのユーザに確認を求めることにより、判別できる。このエンタテインメントシステムは、各エンタテインメント本体装置１が認証用サーバ４に対して接続されていることにより、このような確認作業が可能となる。

【００７６】

Ｎｏ．３及びＮｏ．４の、送信されたディスクＩＤと機器ＩＤの組み合わせの内、ディスクＩＤが未登録の場合、ディスク２の初回使用と判断され、ユーザデータベース５にディスクＩＤが登録される。以下具体的に説明する。

【００７７】

ステップS202において、認証用サーバ４は、ユーザが使用するエンタテインメント本体装置１に対する接続認証を行う。ここで、本体装置１の機器ＩＤが、本体装置１からの送信データの一部として自動的にサーバに供給されるなら、ユーザはユーザＩＤであるパスワードのみを入力すればよい。接続認証に失敗した場合、ステップS203において、ユーザ端末装置と認証用サーバ４の間の接続は遮断される。接続認証が成功すれば、ステップS204において、ユーザの本体装置１との通信接続が確立される。

【００７８】

ステップS205において、認証用サーバ４は、エンタテインメント本体装置１か

らディスクＩＤデータ及び機器ＩＤを受信する。これは図３のステップS109に対応する処理である。

【００７９】

ステップS206において、認証用サーバ４は、受信したディスクＩＤ、機器ＩＤと、ユーザデータベース５に記録されているユーザ情報（ディスクＩＤ、機器ＩＤ）との比較を行う。

【００８０】

ステップS207において、受信したディスクＩＤが、データベース５に登録されたディスクＩＤと一致しているか否かが判定される。即ち、受信したディスクＩＤが、ユーザデータベース５上のテーブルになければ、そのディスクは初回の使用である。この場合はステップS208に進み、認証用サーバ４は、データベース５へのディスクＩＤの登録を行う。そして、ステップS212で、プログラム実行許可命令をエンタテインメント本体装置１に送信する。

【００８１】

送信ディスクＩＤがデータベース５に登録済みであれば、ステップS209に進み、受信機器ＩＤと、前記ディスクＩＤの使用機器として登録された機器ＩＤとが一致しているか否かが判断される。機器ＩＤが不一致の場合、ステップS210に進み、ディスクＩＤに対応する機器ＩＤのユーザ（ディスク所有者）に対して、使用許可の確認をする。ステップS211で、ディスク所有者が承諾すれば（即ち、ディスク所有者が、ディスク使用を許諾する旨をサーバ４に返信すれば）、これはディスク所有者が自分のディスクを他人に貸与したか、他のエンタテインメント本体装置１を利用して実行しているかであり、ステップS212で、プログラム実行許可命令をエンタテインメント本体装置１に送信する。

【００８２】

ディスク所有者が承諾しない場合、不正使用と判断され、ステップS214で不正使用のカウントがなされ、ステップS215で、プログラム実行拒否命令がエンタテインメント本体装置に送信される。これにより、中古品等の不正使用が排除される。

【００８３】

ディスクＩＤと機器ＩＤの組み合わせがユーザデータベース５に登録されているユーザ情報と一致していた場合でも、極めて希なケースであるが両方のＩＤが不正にコピーされた場合には、これを排除する必要がある。ステップS213で、同じ時間帯に同じディスクＩＤ－機器ＩＤの組み合わせでの使用が重複しているか否かが判断される。同時使用が発生していない場合、ステップS212で、プログラム実行許可命令がエンタテインメント本体装置１に送信される。同時使用が発生している場合、不正使用と判断され、ステップS214で不正使用のカウントがなされ、ステップS215で、プログラム実行拒否命令がエンタテインメント本体装置に送信される。

【００８４】

通常、不正ディスクは真正なディスク内容をそのままコピーするため、データエリアに記録されたディスクＩＤのアドレスデータもコピーされてしまう。しかし、本実施の形態のフォーマットにおける、リードインエリアの内側又はリードアウトエリアの外側等のデータエリア以外に記録されたＩＤ情報は、真正ディスクをそのままコピーした不正ディスクにはコピーされない。これにより、不正ディスクにはディスクＩＤのアドレスに関する情報はコピーされているにもかかわらず、ディスクＩＤ自体が存在しないので、不正ディスクに対しては、図３のステップS104でディスクＩＤのアドレス有りと判定され、次いでステップS106でディスクＩＤ自体なしと判定されることにより、ステップS107でプログラムの実行が排除されることとなる。

【００８５】

ディスクＩＤの記録方法は、上述の方法に限定されない。例えば、ディスクＩＤは、データエリア内に、ピット列の物理的な変動を利用した方法で形成することも出来る。このピット列の物理的な変動を利用した方法は、ピット列の半径方向の変動（ウォブリング）、ピットサイズの短径方向の変動又はピットの深さ方向の変動のいずれかを利用することが出来る。或いは、ディスクＩＤは、電子透かし(Digital Wat rmark)を利用した方法で形成することも出来る。

【００８６】

認証用サーバへのディスクＩＤの登録方法は、上述の方法に限定されない。な

お、特別な場合として、例えば光ディスク等の記録媒体の提供者自身が認証用サーバ４を提供するような場合がある。この場合には、自ら製造・提供するディスクＩＤは、予め認証用サーバ４のデータベース５に登録・蓄積しておくことが出来る。このような場合、第１のディスクＩＤ認証システムでは、初回使用時のディスクＩＤの登録処理は不要となる。

【００８７】

また、機器ＩＤは必ずしも必要でない。機器ＩＤは各々のユーザ固有のユーザＩＤで置き換えることが出来る。即ち、使用機器を特定する代わりに、ユーザを特定し、ユーザＩＤとディスクＩＤとの組み合わせにより、認証システムを機能させることが出来る。この場合、好ましくは、ユーザＩＤはパスワードの形式で付与される。

【００８８】

光ディスク等の記録媒体の提供者自身が認証用サーバ４を提供するような場合について、更に説明する。

【００８９】

この記録媒体提供者が、ディスク製造時に、ディスク一枚毎に個別の製造番号を与え、これをディスクＩＤとしてディスク２内に情報として組み込む。同時に、ユーザデータベース５には、そのディスクＩＤ（製造番号）が記録されている。一方で、エンタテインメント装置１の製造時に、エンタテインメント装置一台毎に個別の製造番号を与え、これをエンタテインメント装置内に機器ＩＤとして組み込まれている。そして同時に、ユーザデータベース５には、その機器ＩＤ（製造番号）が記録されている。

【００９０】

この場合、ディスク２の工場出荷時には、ディスクＩＤは、エンタテインメント装置１の機器ＩＤと未だ関連付けられていない。

【００９１】

ディスク２の利用者が、認証用サーバ４に対して接続・認証処理の要求を行う（S109）と、認証用サーバ４は機器ＩＤ認証後に、ディスクＩＤの認証を行う。

【００９２】

ユーザデータベース５には、予め機器ＩＤ，ディスクＩＤ（ユーザ情報）が記録されているので、認証用サーバ４はエンタテインメント装置１から受信した機器ＩＤ－ディスクＩＤがこのユーザデータベース５に記録されたユーザ情報に該当するか否かをチェックする。

【００９３】

その結果、ユーザデータベース５のユーザ情報に該当するものがなかった場合には、認証を強制終了してディスク２のプログラム実行を拒否する。この際、不正なディスクＩＤをユーザデータベース５に蓄積するようにしておけば、各エンタテインメント装置毎の不正なディスクを利用しての認証用サーバ４へのアクセス回数のカウントや、不正ディスクを利用したエンタテインメント装置１の特定等の不正ディスクに関わる管理が可能となる。

【００９４】

また、不正なディスクの排除以外に関しても、ディスクＩＤが付与されたディスク２を用いたアクセス回数のカウントは、本発明のネットワークシステムにおいて有効に利用することが可能である。即ち、認証用サーバ４へのアクセス回数を利用して、アクセス回数がある回数以上に達した時、認証を強制終了してディスク２のプログラム実行を拒否するようにすることも出来る。

【００９５】

例えば、ＩＤが付与されたディスク２を用いた認証用サーバ４へのアクセス回数を管理することで、ディスク２に含まれるプログラム等のコンテンツに対しお試し期間を設けてユーザに利用させることが可能である。これにより、ユーザはあるディスク２の利用回数がある一定回数に達するまでは、お試し期間としてディスク内のプログラム等のコンテンツを利用してゲームやサービス等を利用することが可能である。

【００９６】

現在、多くのインターネット接続サービス体験版ソフトは、利用時間をカウントすることでお試し期間を設けているが、本発明のネットワークシステムを用いれば、サービスの利用時間による管理ではなく利用回数による管理が可能となる。

【００９７】

例えば、音楽や映像を、本発明の認証用サーバ４を介してコンテンツサーバ６からエンタテインメント装置１に対してダウンロード提供するサービスに利用可能である。ここで、サービスに加入したユーザは、サービス提供者からサービス利用のためのディスク２を配布されるものとする。ディスク内には、ディスク毎に付与されたディスクＩＤと共に、認証用プログラム、ダウンロード実行用プログラム等が記録されている。ユーザは、このディスク２をエンタテインメント装置１に装着することで認証用サーバ４並びにコンテンツサーバ６に接続することが可能となり、これにより音楽や映像等をダウンロード可能となる。

【００９８】

この際、ダウンロード回数をディスクＩＤを付与したディスク２を用いたコンテンツサーバ６へのアクセス回数として認証用サーバ４がカウントすれば、ダウンロード（通信）時間に依存しない、サービスの利用回数制限が実現可能となる。

【００９９】

更に、認証用サーバ４においてユーザがアクセスしたコンテンツ内容を表す情報とユーザ情報（機器ＩＤ，ユーザＩＤ，ディスクＩＤ等）とを相互に関連付けてユーザデータベース５内に蓄積していけば、ユーザ毎の嗜好等を容易に管理することが可能となる。これらの蓄積情報を用いて、サービス提供者或いはコンテンツ提供者は各ユーザ毎に適切な広告等をインターネット等の通信回線を通じて提供することが可能となる。

【０１００】

以上は利用回数に応じた、サービス提供等の利用制限方法であったが、制限方法はこれに限られない。例えば、ディスクＩＤが付与されたディスク２に記録された内容を、サービス提供者がユーザからの徴金状況に応じて、制限を付けて提供することもできる。ディスク２に記録された内容は、すべてを利用可能ではなく部分的に利用可能であるとする。ユーザが、その部分的に利用ができない内容を利用したい時には、ユーザはその利用内容に応じた対価をサービス提供者に支払うこととなる。サービス提供者は、それを受けて、ユーザによる利用を可能と

する。

【０１０１】

例えば、ディスク２に記録された内容を部分的に暗号化しておけば、利用対価を支払わないユーザは暗号部分に相当する利用できないが、利用対価を支払ったユーザに対しては、暗号を解読するための鍵をサービス提供者からユーザのエンタテインメント装置１に提供を行うことで、利用可能となる。前記サービス提供者からエンタテインメント装置１に対して送信される情報は、暗号解読用の鍵には限られない。

【０１０２】

また、ユーザがディスク２の部分的に利用できない記録内容を利用するためにサービス提供者に対して行うのは、対価の支払いに限られず、例えばユーザのエンタテインメント装置１からサービス提供者が運営する認証用サーバ４への、ユーザＩＤの送信であってもよい。このユーザＩＤは、サービス提供者から各ユーザに対して予め付与されたＩＤであってもよい。

【０１０３】

（第２のディスクＩＤ認証システム）

次に、第２のディスクＩＤ認証システムについて説明する。第２のディスクＩＤ認証システムでは、認証対象となるディスクは、ＣＤ－ＲＯＭ等に限定されず、ＴＯＣの規定されていないＤＶＤ－ＲＯＭ等も含められる。また、ディスク内のディスクＩＤの記録箇所も限定されておらず、リードインエリアの内側、リードアウトの外側、又はデータエリア内のいずれの箇所であってよい。

【０１０４】

上記第１のディスク認証システムと比較すると、第１のディスク認証システムでは、ゲームをプレーするためにディスク上のプログラムを起動する毎に、サーバに接続して認証を行っていたが、この第２のディスク認証システムでは、ユーザ情報をメモリカード１１等の本体接続型の外部記憶装置に記憶することで、サーバに接続する処理行程を省略している。即ち、ディスクの初回使用時に、メモリカード１１等にディスクＩＤ－機器ＩＤのユーザ情報を記録し、ゲーム実行毎にこのユーザ情報を利用してディスクの認証を行っている。なお、外部記憶装置

には、アプリケーションプログラム等のコンテンツが記録されていてもよい。

【０１０５】

図５を用いて第２のディスクＩＤ認証システムのエンタテインメント本体装置側の処理について具体的に説明し、図６を用いて認証用サーバ４側の各ステップでの処理内容について具体的に説明する。

【０１０６】

ステップS302で、エンタテインメント本体装置１は、ＣＰＵ１６の制御の下、装着ディスク２に記録されている固有の基礎データをメインメモリ１７に読込む。装着ディスク２は、ＣＤ、ＣＤ－ＲＯＭ、ＤＶＤ－Ｖｉｄｅｏ、ＤＶＤ－ＲＯＭ等の各種ディスクが含まれる。

【０１０７】

ステップS303では、読み込んだ基礎データの中にディスクＩＤが有るか否かが判断される。ディスクＩＤが存在しなければ、認証対象以外のディスクであると判断され、ステップS312に進み、プログラムが実行される。

【０１０８】

ディスクＩＤが存在する場合、ステップS304に進み、ＣＰＵ１６の制御の下、エンタテインメント本体装置に接続されたメモリカード１１等の外部記憶装置に記録されたユーザ情報（ディスクＩＤ－機器ＩＤの組み合わせデータ）が読み込まれる。なお、このメモリカード１１等には、ゲームのハイスコア、前回中断したゲームの進行状況のバックアップデータ等のデータも記録されている。

【０１０９】

ステップS305では、メモリカード１１にディスクＩＤが記録されているか否かが判断される。ディスクを最初に使用した時に、メモリカード１１のユーザ情報にディスクＩＤと機器ＩＤとが登録されるため、２回目以降の使用時には、メモリカード１１に、ディスクＩＤがユーザ情報として記録されていることになる。従って、メモリカード１１にディスクＩＤの記録が無い場合としては、①ディスクの初回使用時、②メモリカード自体の交換時、等が考えられる。読み取ったディスクＩＤがメモリカード等に記録されていた場合、ステップS306に進む。

【０１１０】

ステップS306では、メモリカード１１等に記録されているディスクＩＤが、装着ディスクのディスクＩＤと一致するか否かが判断される。一致しない場合としては、ディスクの初回使用時その他が考えられる。一致していれば、ステップS307に進む。

【０１１１】

ステップS307において、メモリカード１１から読み込んだ機器ＩＤが、現在使用している本体装置の機器ＩＤと一致するか否かが判断される。一致しない場合としては、ディスク所有者からディスク２とメモリカード１１とを借りてきたユーザが、自らの本体装置でゲームをする場合等が考えられる。一致する場合（ディスクＩＤ－機器ＩＤの組み合わせが、ディスク購入時にメモリカード等に記録したユーザ情報と一致している場合）、正当使用に該当し、ユーザ認証を完了して、ステップS312でプログラムが実行される。

【０１１２】

ステップS305で、メモリカードにディスクＩＤが存在しなかった場合、ステップS306で、メモリカード１１等に記録されているディスクＩＤがディスクから読み込んだディスクＩＤと一致しなかった場合、又はステップS307で、メモリカード１１等に記録されている機器ＩＤが使用機器の機器ＩＤと一致しなかった場合は、ステップS308に進む。このステップS308で、エンタテインメント本体装置は、ＵＳＢ、ＩＥＥＥ１３９４、ＰＣＭＣＩＡ等の通信インターフェイスを介して、ディスクＩＤ、使用機器の機器ＩＤデータを認証用サーバ４に対して送信し、ステップS309でユーザ認証を待つ。この後、認証用サーバ４から、これらのディスクＩＤ、機器ＩＤデータをメモリカード１１に記録する命令を受信したときは、これらの書き込みを行う（図６のステップS405に対応）。

【０１１３】

ステップS310で、認証用サーバ４での認証処理結果を元にプログラムの実行の可否を決定する。「認証否」の場合、ステップS311に進み、プログラムの実行が拒否され、強制終了される。「認証適」の場合、ステップS312に進み、プログラムを実行する。

【０１１４】

図６は、第２のディスクＩＤ認証システムにおける認証用サーバ４側の処理内容を示している。

【０１１５】

ステップS402で、認証用サーバ４は、エンタテインメント本体装置に対する接続を確立した後、ディスクＩＤ、本体装置の機器ＩＤを受信する。ディスクＩＤは、図５のステップS302でディスクから読み取られ、ステップS308で送信されたディスクＩＤであり、機器ＩＤもステップS308で送信されたものである。

【０１１６】

ステップS403で、受信したディスクＩＤが認証用サーバ４のユーザデータベースに蓄積されているディスクＩＤの中に存在するか否かが判定される。存在しない場合、そのディスクは初回使用と判断される。従って、ステップS404で、受信したディスクＩＤ－機器ＩＤの組み合わせが、ユーザデータベース５にユーザ情報としてテーブル化して蓄積（登録）される。次いで、ステップS405で、ディスクＩＤ－機器ＩＤを互いに関連付けてユーザの本体装置１に接続されているメモリカード１１等に記録させることで、図５で説明した認証処理を可能とする。

【０１１７】

ステップS406で、認証用サーバ４は、使用ディスクに対するパスワードを本体装置１に送信する。このパスワードは、ディスクの所有者しか知り得ない秘密キーであり、後述するように、ユーザの意思確認のために使用される。このパスワードは、ユーザが使用する本体装置１の画面に対して出力されることが好ましい。ユーザはこのパスワードを書き留めておくことにより、他人へディスクを貸出すときにパスワードを教え、その他人がディスクを使用できるようにすることが可能となる。その後、ステップS414で、エンタテインメント本体装置に対してプログラム実行許可命令を送信する。

【０１１８】

ステップS403で、受信ディスクＩＤが、登録されているディスクＩＤと一致した場合、ステップS407で、受信した機器ＩＤが、前記ディスクＩＤに対応するデータベース中の機器ＩＤと一致するか否かが比較され、ステップS408で、両者が一致するか否かが判定される。一度でも使用されたディスクに関しては、ユーザ

データベース５にディスクＩＤ－機器ＩＤの組み合わせからなるデータが蓄積されているため、このステップS408においては、機器ＩＤがディスクＩＤに対応するものであるか否かを判別する。これにより、中古使用を排除することが出来る。メモリカード１１の交換、メモリカードのディスクＩＤ－機器ＩＤの記録の消失等の場合、ステップS409で、認証用サーバ４は、ディスクＩＤ－機器ＩＤの組み合わせデータをエンタテインメント本体装置に送信してメモリカードに記録させる。その後、ステップS414で、エンタテインメント本体装置に対してプログラム実行許可命令を送信する。

【０１１９】

ユーザデータベース５にディスクＩＤは存在するが、対応機器ＩＤがデータベース中のものと一致しない場合、ステップS408からステップS410に進み、パスワードの入力要求をエンタテインメント本体装置１に送信する。この入力要求は、本体装置１に接続されたテレビジョンモニタ（図示せず。）に表示される。ステップS411で、ユーザから受信したパスワードが、正当か否かが判断される。正当であれば、ステップS412に進み、このディスクの借用者等に新たなパスワードを発行して送信する。ディスク借用者等がディスク所有者からディスクを合意のもとで借りるとき、このパスワードを入力することで、プログラム実行拒否命令を回避することが可能となる。この結果、ディスク借用者は、必ずしもディスク所有者から、ディスク２と共にメモリカード１１を借りる必要が無くなる。また、ステップS412では、ディスク所有者に対して発行したディスク固有のパスワードを更新する。更新したパスワードはディスク所有者に対して送信される。これにより中古品の蔓延を助長することが回避できる。

【０１２０】

ステップS412の後、ステップS414で、認証用サーバ４は、エンタテインメント本体装置に対してプログラム実行許可命令を送信する。

【０１２１】

ステップS411で、ユーザから受信したパスワードが正当ではないと判断された場合は、ステップS413に進み、認証用サーバ４からエンタテインメント本体装置に対して、プログラム実行拒否命令が送信される。

【０１２２】

上述した第１のディスクＩＤ認証システム及び第２のディスクＩＤ認証システムの実施例では、ユーザは、自分のエンタテインメント装置１に対して、手許にある光ディスクのような記録媒体からプログラムを読み込んでいる。しかし、本発明はこれに限定されない。例えば、ディスクＩＤが付与された記録媒体が他所にあり、遠隔操作により第１又は第２のディスクＩＤ認証システムを実行して認証許可を得た後で、その記録媒体に記録されたプログラムをダウンロードすることも出来る。或いは、例えば、ディスクＩＤが付与された記録媒体が他所にあり、その記録媒体に記録されたプログラムをダウンロードした後で、第１又は第２のディスクＩＤ認証システムを実行して認証許可を得て、プログラムを実行することも出来る。

【０１２３】

【発明の効果】

本発明によれば、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムを有するコンピュータシステムを提供することができる。

【０１２４】

更に、本発明によれば、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムを有するコンピュータシステムの使用方法を提供することができる。

【図面の簡単な説明】

【図１】

図１は、ディスクＩＤ認証システムを説明する図である。

【図２】

図２は、図１のエンタテインメント本体装置の構成を示す図である。

【図３】

図３は、第１のディスクＩＤ認証方法における本体装置側の処理のフローである。

【図４】

図４は、第１のディスクＩＤ認証方法における認証用サーバ側の処理のフロー

である。

【図５】

図５は、第２のディスクＩＤ認証方法における本体装置側の処理のフローである。

【図６】

図６は、第２のディスクＩＤ認証方法における認証用サーバ側の処理のフローである。

【図７】

図７は、認証用サーバが受信したディスクＩＤ及び機器ＩＤと、ユーザデータベースに予め蓄積されたユーザ情報との比較結果を表す表である。

【符号の説明】

１：エンタテインメント本体装置（コンピュータ）

２：光ディスク（第１の記録媒体）

４：認証用サーバ

５：ユーザデータベース

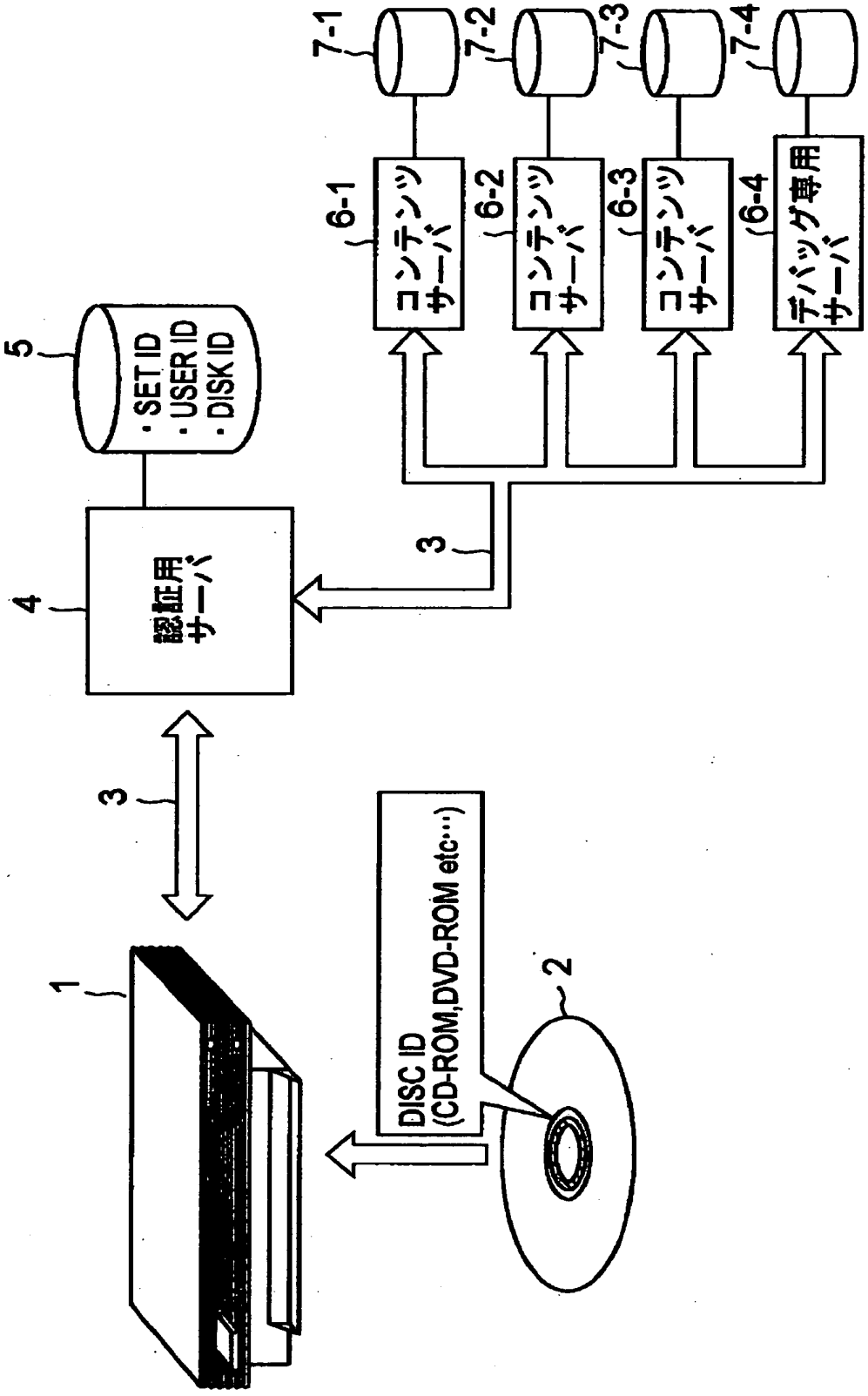
６：コンテンツサーバ

７：データベース

１１：メモリカード（第２の記録媒体）

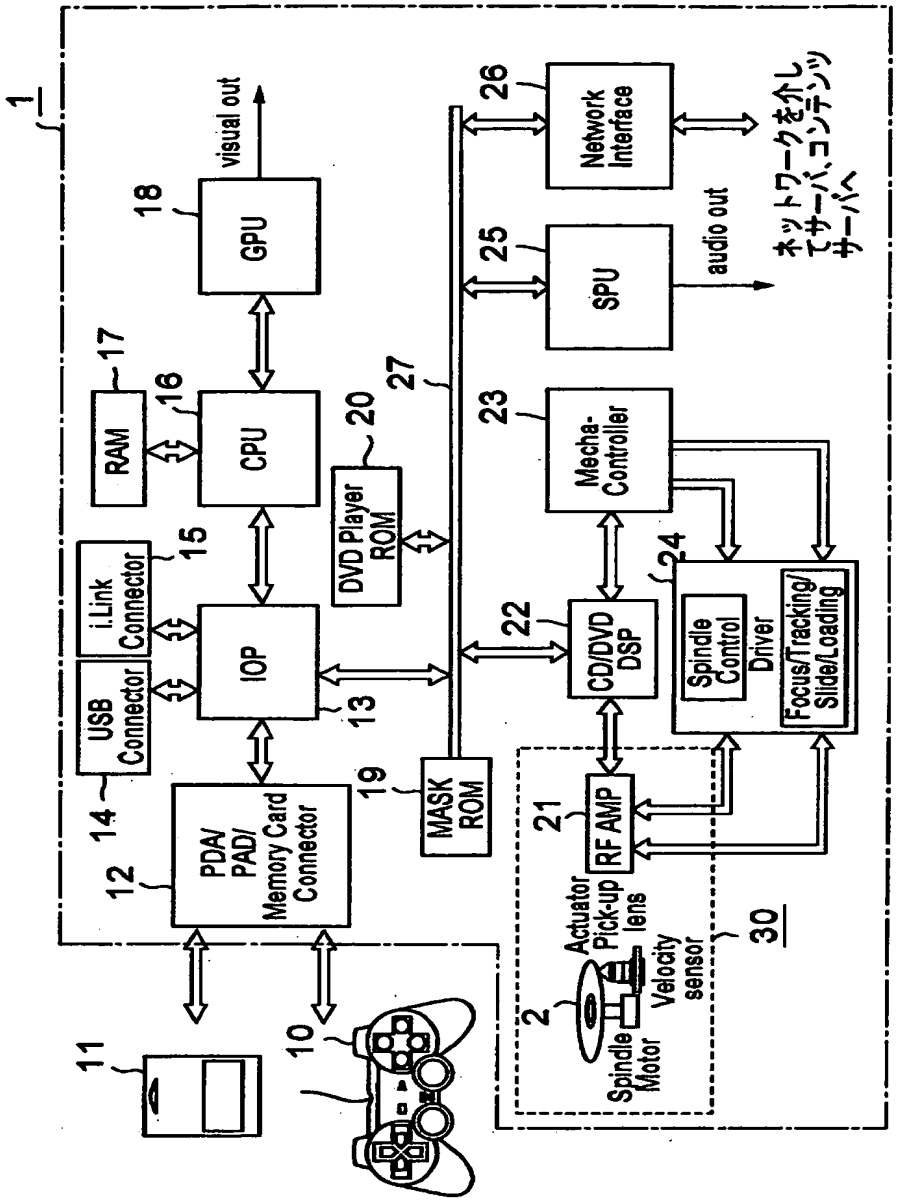
【書類名】　　図面

【図１】



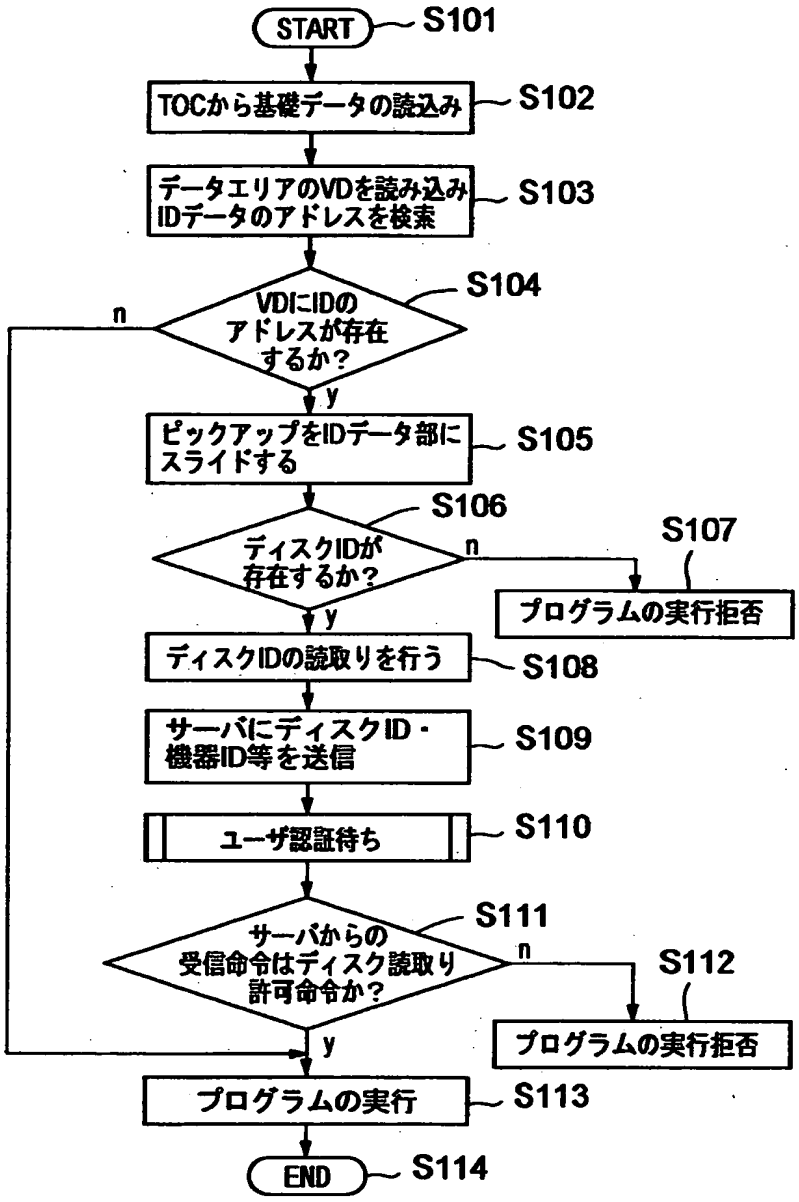
システムの概念図

【図２】



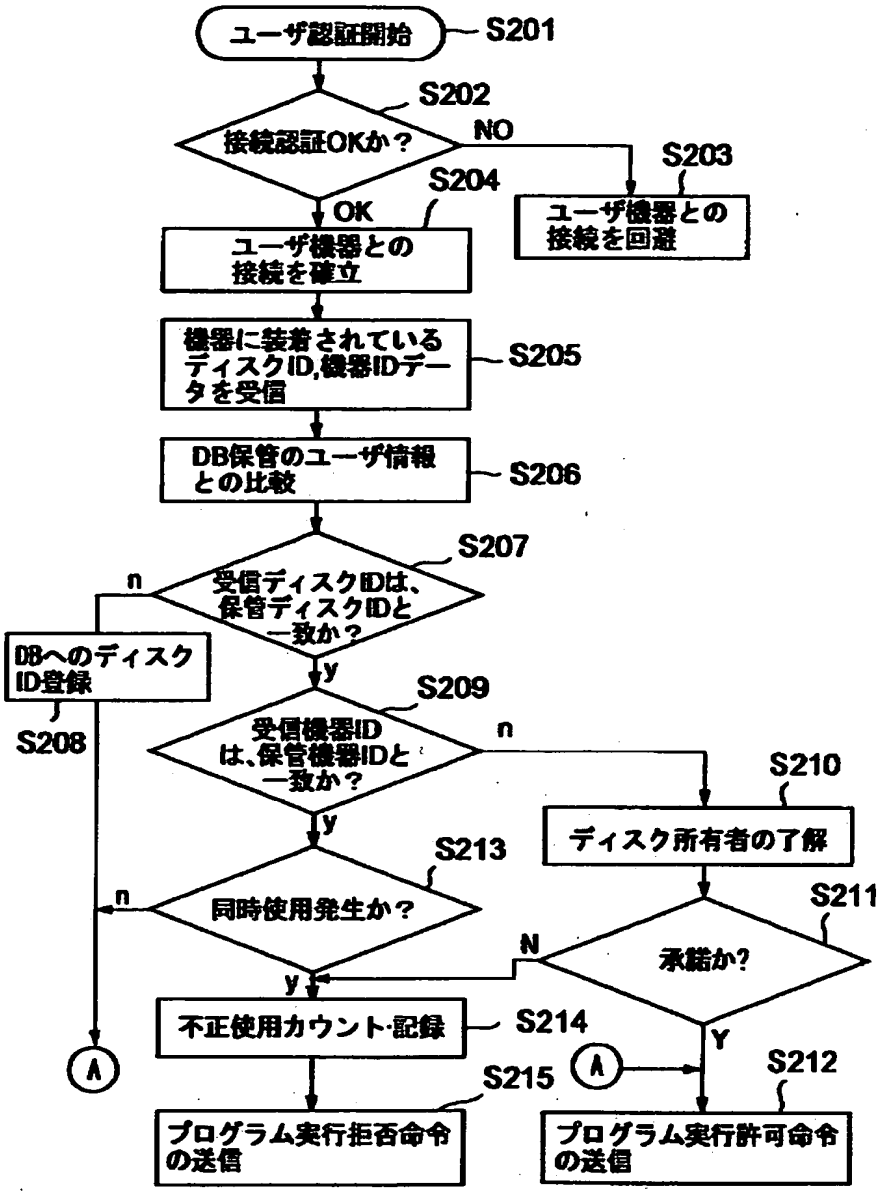
エンタテイメント本体装置の構成

【図３】



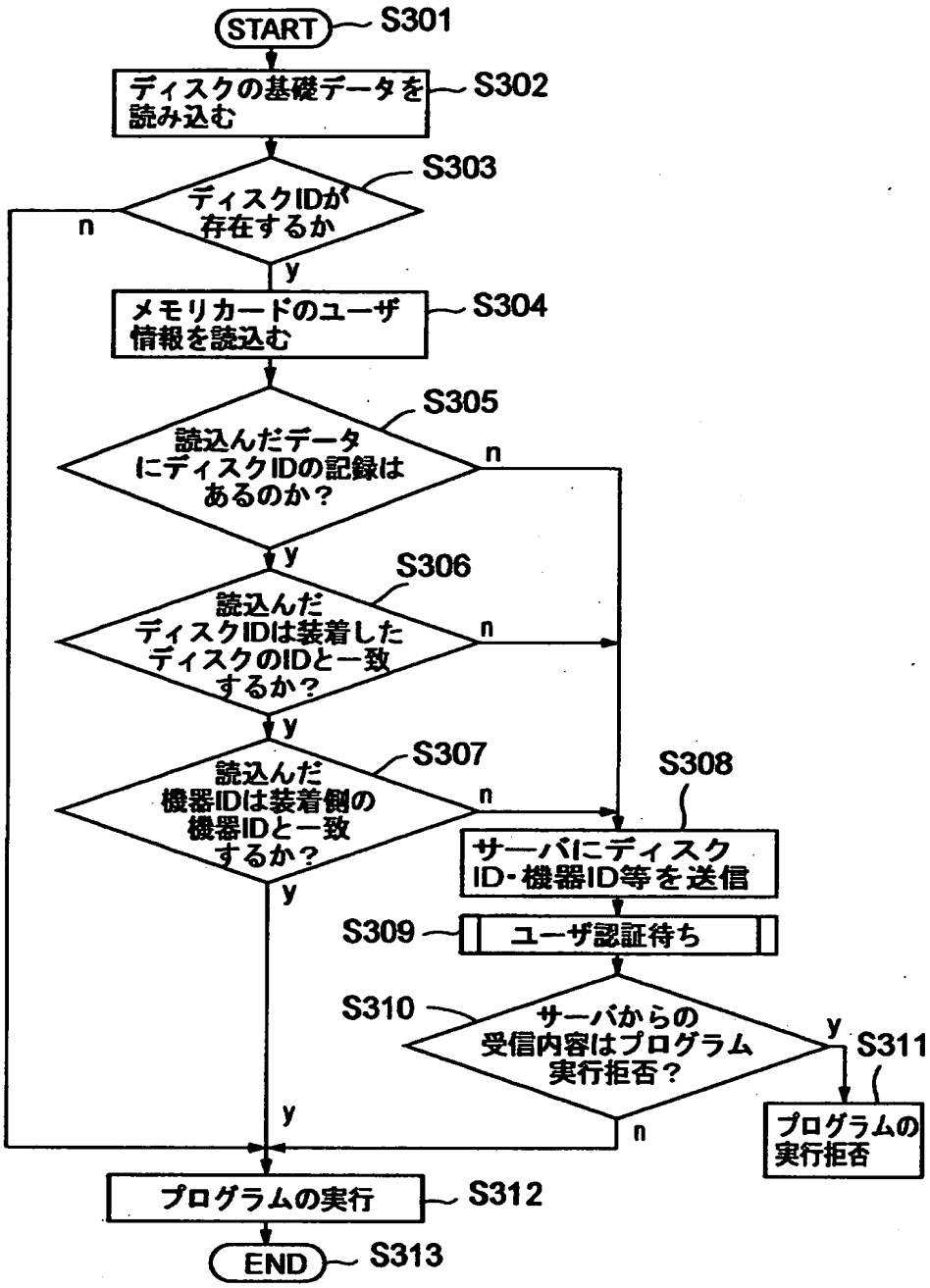
ディスクID認証（本体装置側処理）

【図４】



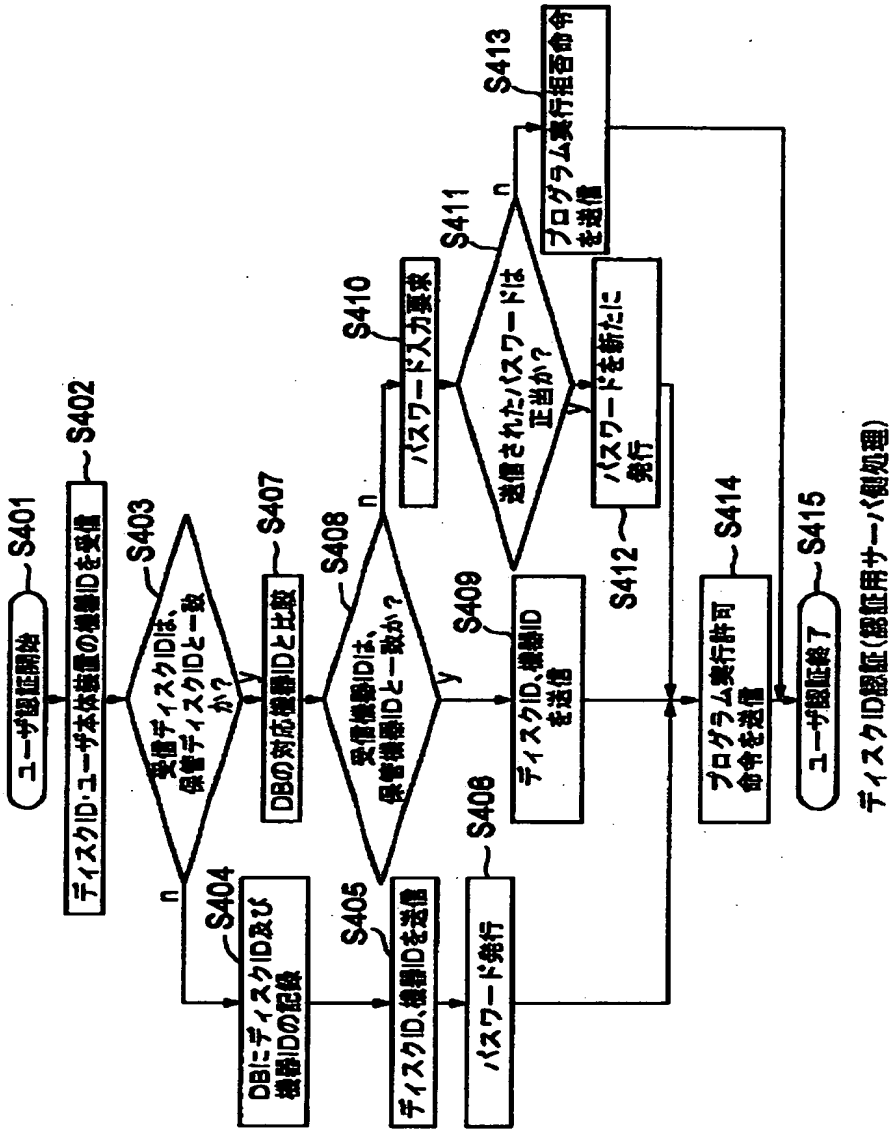
ディスクID認証(認証用サーバー側処理)

【図５】



ディスクID認証(本体側処理)

【図６】


S401
ユーザ認証開始
S402
ディスクID・ユーザ本体装置の機器IDを受信
S403
受信ディスクIDは、保管ディスクIDと一致か？
y
n
S404
DBにディスクID及び機器IDの記録
S405
ディスクID、機器IDを送信
S406
パスワード発行
S407
DBの対応機器IDと比較
S408
受信機器IDは、保管機器IDと一致か？
y
n
S409
ディスクID、機器IDを送信
S410
パスワード入力要求
S411
送信されたパスワードは正当か？
y
n
S412
パスワードを新たに発行
S413
プログラム実行拒否命令を送信
S414
プログラム実行許可命令を送信
S415
ユーザ認証終了
ディスクID認証（認証用サーバ側処理）

【図７】

No.	送信情報	蓄積されたディスクＩＤ	蓄積された機器ＩＤ
1	送信ディスクＩＤ，送信機器ＩＤ	○	○
2		○	×
3		×	○
4		×	×

【書類名】　　要約書

【要約】

【課題】　光ディスクが不正使用されているか否かを検証する認証システムを有するコンピュータシステム

【解決手段】　光ディスクが夫々装着可能な複数のコンピュータがネットワークを介して認証用サーバに接続可能なコンピュータシステムであって、各々の前記コンピュータは固有の機器ＩＤを有し、各々の前記光ディスクは固有のディスクＩＤを有し、前記サーバは、前記コンピュータの使用時に前記機器ＩＤを、前記光ディスクの使用時にディスクＩＤを、夫々蓄積するユーザデータベースを有し、該ユーザデータベースにはディスクＩＤ－機器ＩＤの組のデータが蓄積されており、前記光ディスクの２回目以降の使用時には、前記コンピュータから前記ネットワークを介してディスクＩＤデータと機器ＩＤデータとを認証用サーバに送信し、正当な使用であることを認証する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔３９５０１５３１９〕

１．変更年月日　　１９９７年　３月３１日
［変更理由］　住所変更
住　所　東京都港区赤坂７－１－１
氏　名　株式会社ソニー・コンピュータエンタテインメント